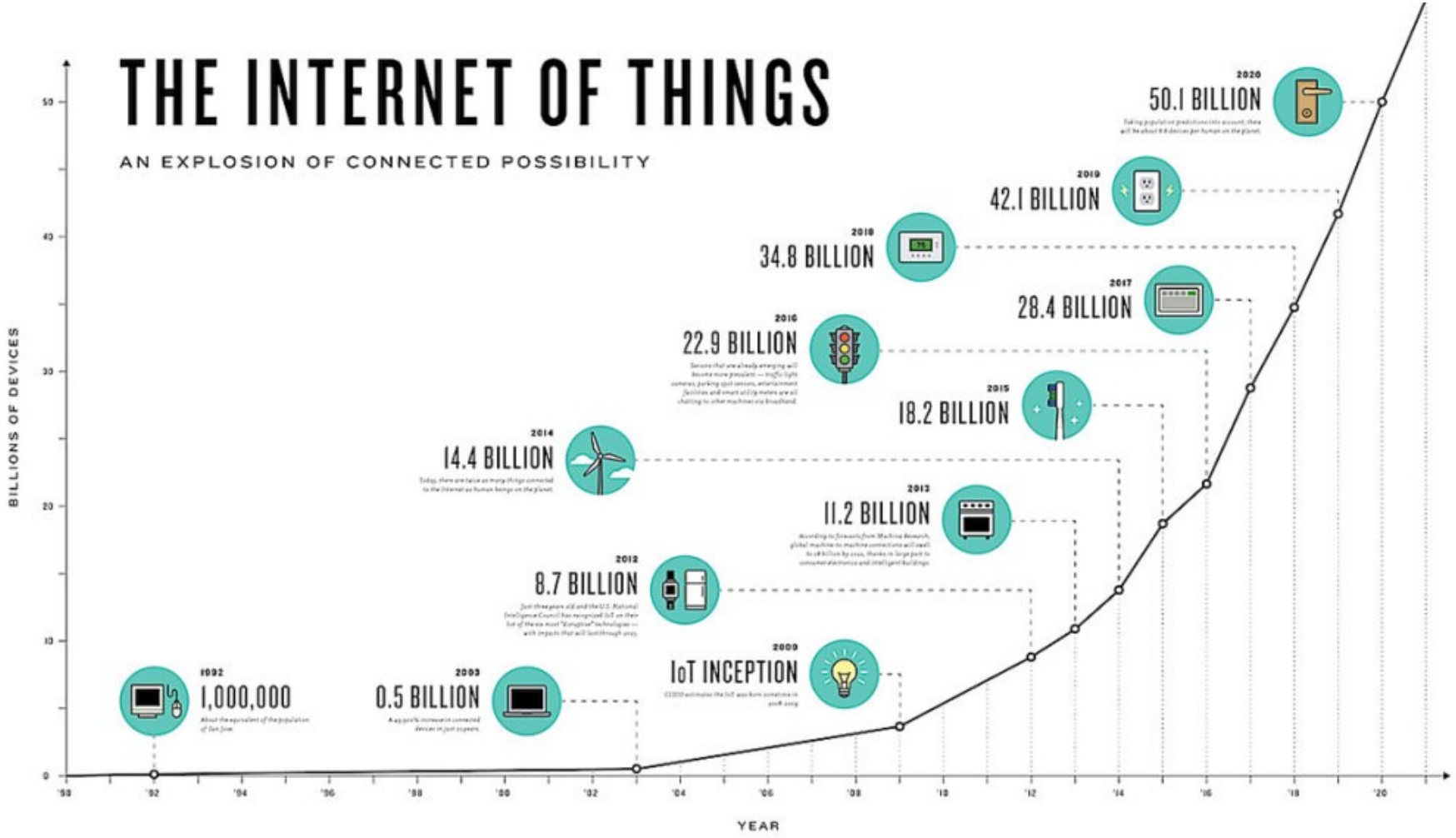
浙江大學
ZHEJIANG UNIVERSITY

ANALOG SECURITY OF CYBER-PHYSICAL SYSTEMS—FROM 0101 TO MIXED SIGNALS

Wenyuan Xu
Zhejiang University

27TH USENIX SECURITY SYMPOSIUM

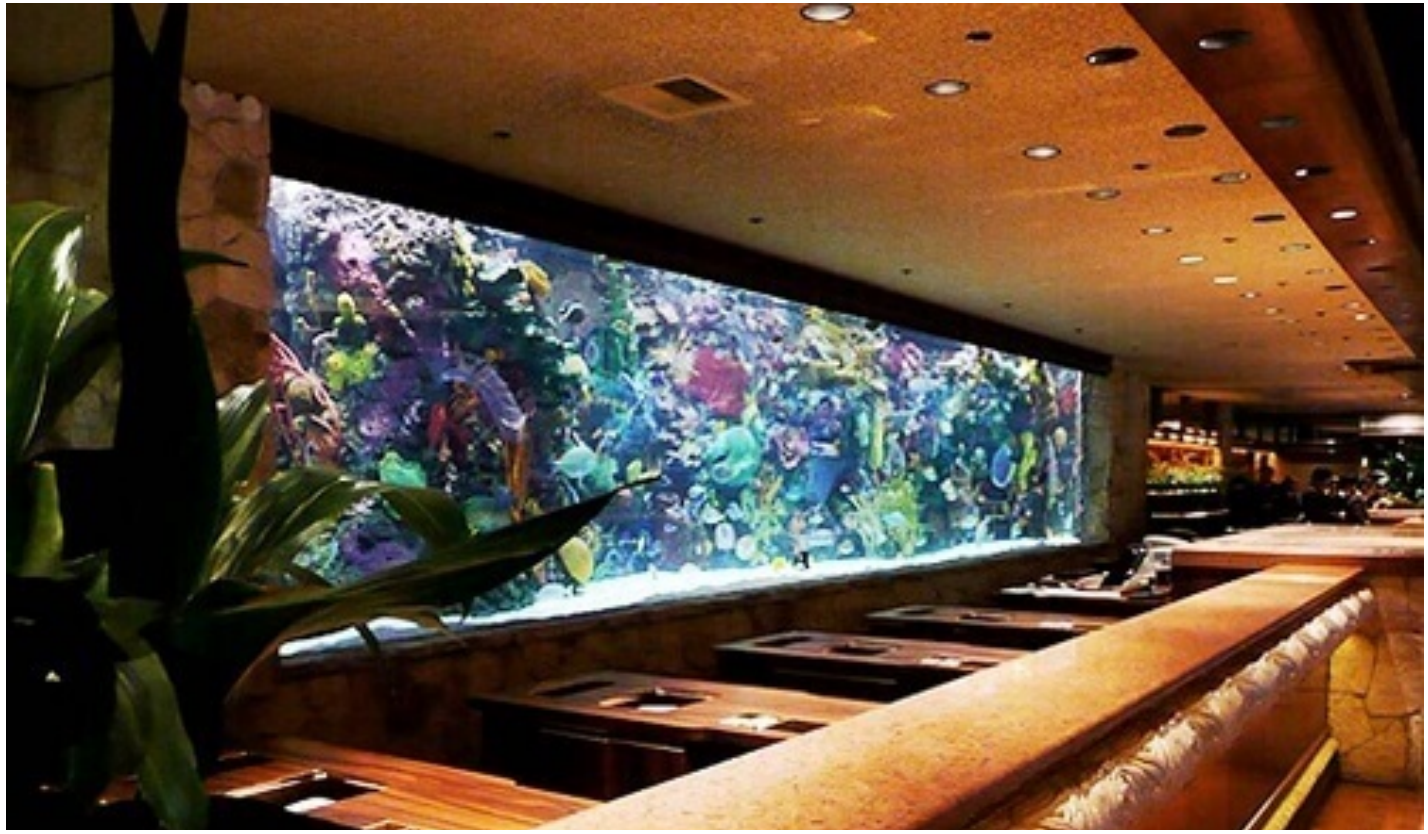
智能系统安全实验室
UBIQUITOUS SYSTEM SECURITY LAB.


THE INTERNET OF THINGS
AN EXPLOSION OF CONNECTED POSSIBILITY
BILLIONS OF DEVICES
YEAR
1992
1,000,000
2003
0.5 BILLION
2009
IoT INCEPTION
2012
8.7 BILLION
2013
11.2 BILLION
2014
14.4 BILLION
2015
18.2 BILLION
2016
22.9 BILLION
2017
28.4 BILLION
2018
34.8 BILLION
2019
42.1 BILLION
2020
50.1 BILLION


11903
11869
11904
11811
11816
11883
11862
11890
11886
11852
11911
11845

CNN tech

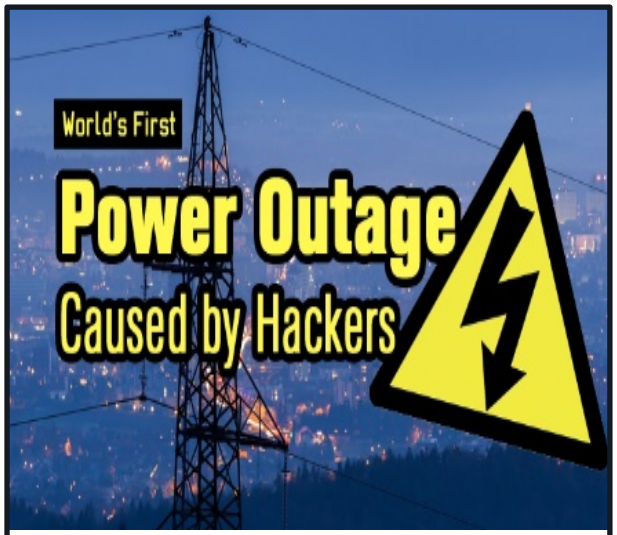
A smart fish tank left a casino vulnerable to hackers



Security Incidents of IoT

Stuxnet → PLC

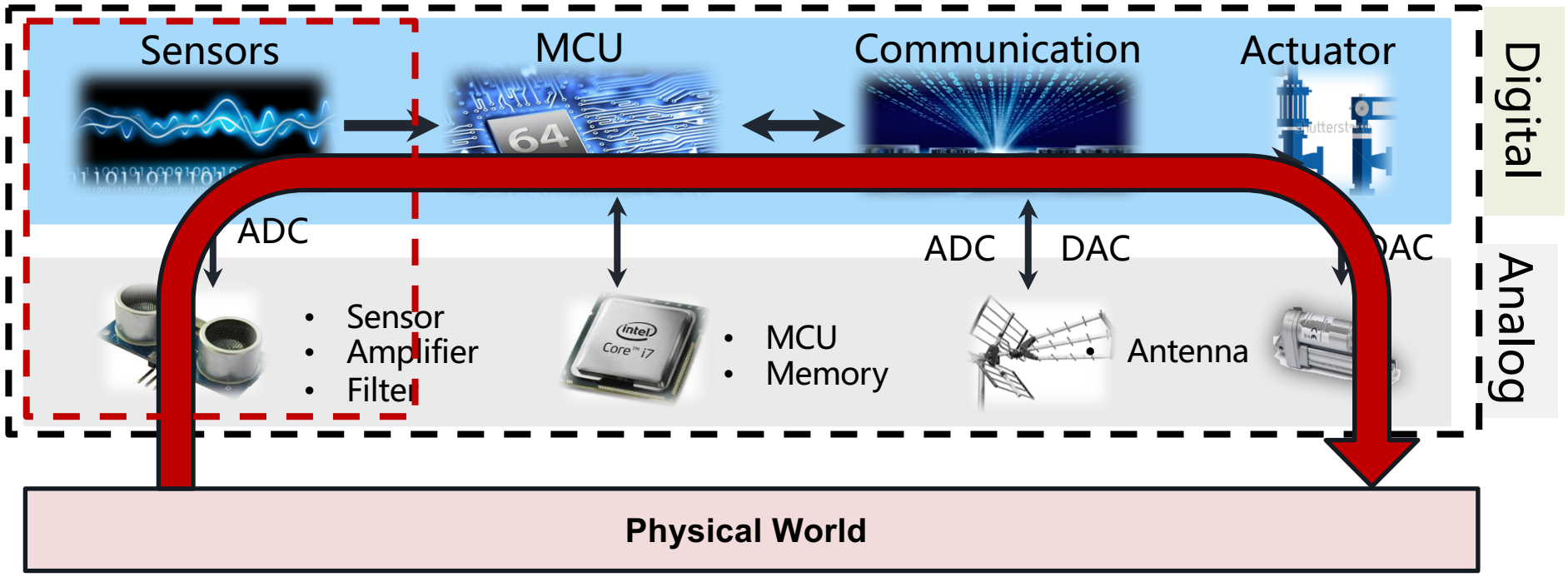
Delayed Iran's nuclear program



Black Energy→ Power grid

Power outage at Ukraine

What is new? → Smart devices

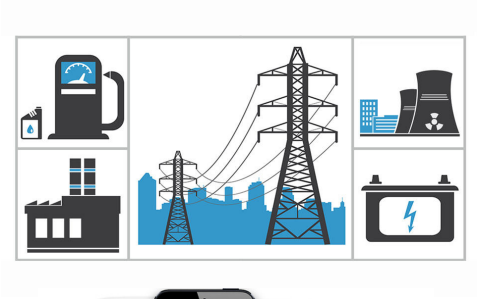


It's time to look at the physics of cybersecurity!

Sensors

Sensors are every where

- Smartphone: >14 sensors
- Car: 60-100 sensors now; 200 in the future.



Accidental interference

Cellphone + Oven

New York Times
Aug 21 2009

Sensors are a proxy for reality

COMMUNICATIONS OF THE ACM | FEBRUARY 2018

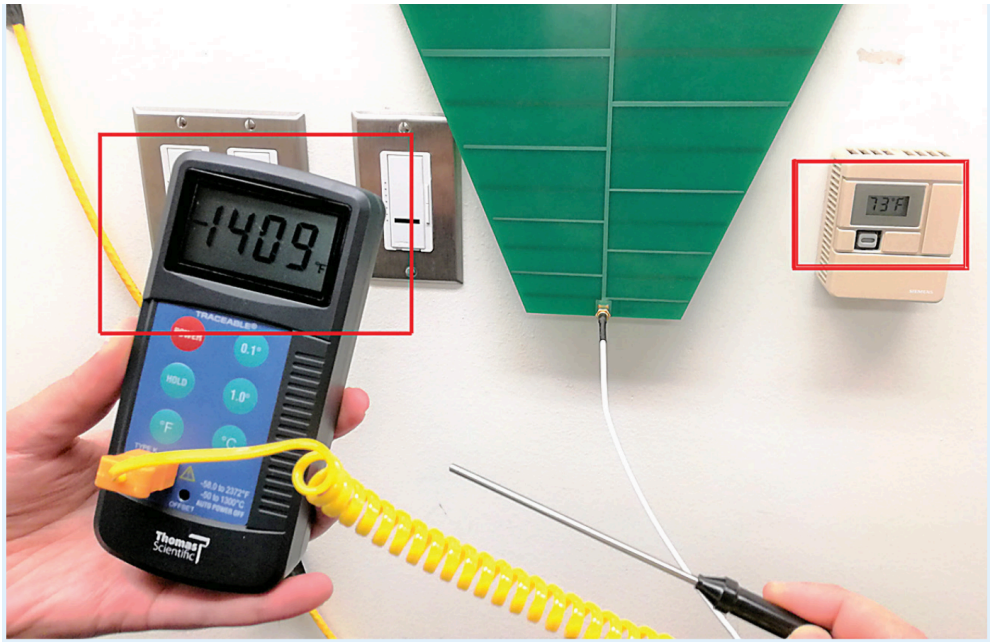
DOI:10.1145/3176402

Inside Risks

Risks of Trusting the Physics of Sensors

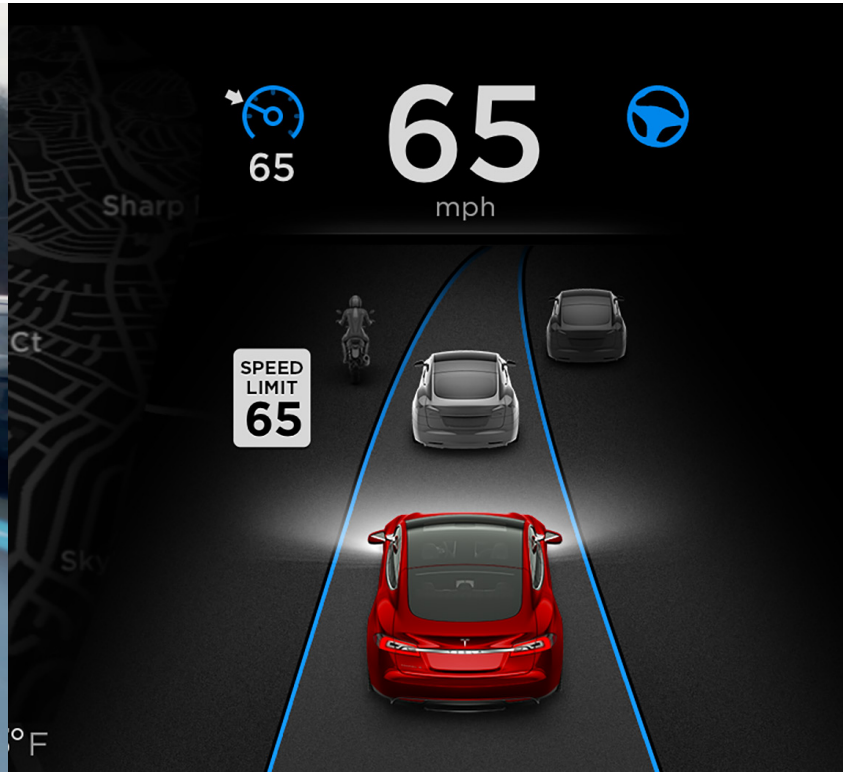
Protecting the Internet of Things with embedded security.

- **Thermocouple interpolates from a voltage potential**
- **Not necessarily temperature**

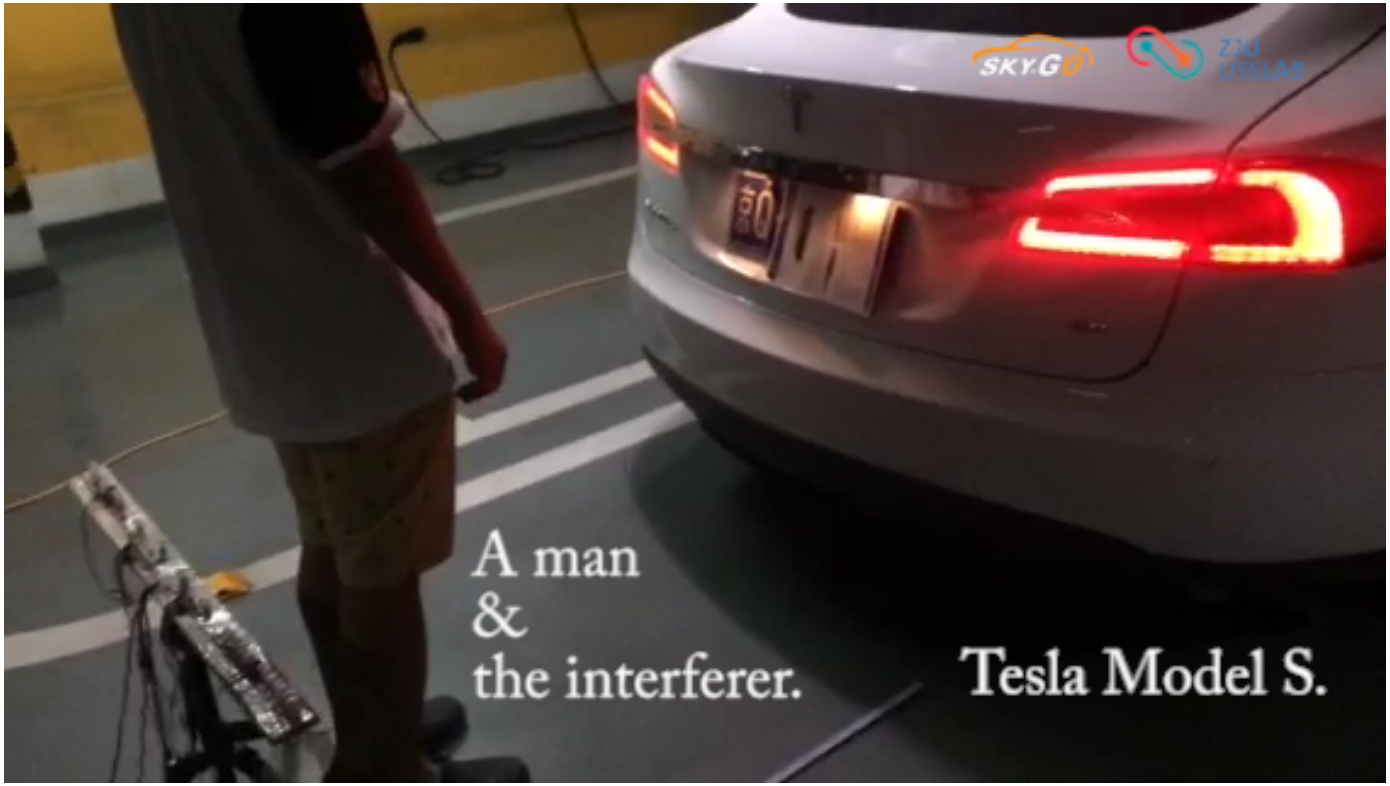


How will a system behave when sensors go wrong?

Tesla Autopilot



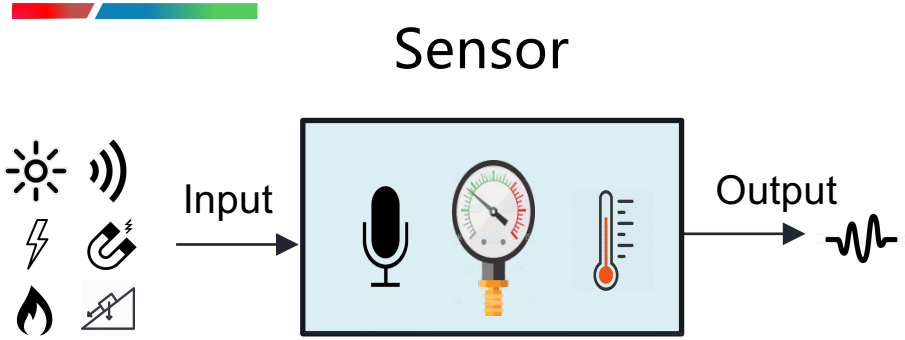
Fooling Obstacle Sensors – Demo on Tesla Summon



How to do research in sensor security?

- Is there a generic sensor model?
- Can we affect the integrity of sensors from outside?
- What's the status quo of sensors in terms of programming/systems?
- How to protect the integrity of sensors?

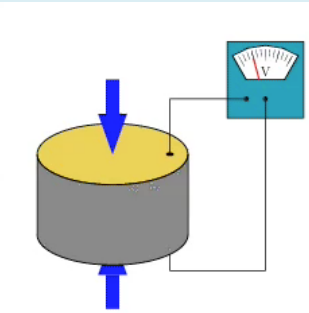
What is inside a sensor module



Physical signals -> Sensor -> Electrical signal

- Electromagnetic -> electrical [Electromagnetic induction]
- Mechanical -> electrical [Piezoelectricity]
- Radiant -> electrical [Photoconductivity]
- Magnetic -> electrical [Hall effect]
- Thermal -> electrical [Seebeck effect]
- Chemical -> electrical [Voltaic effect]

Piezoelectric Sensor

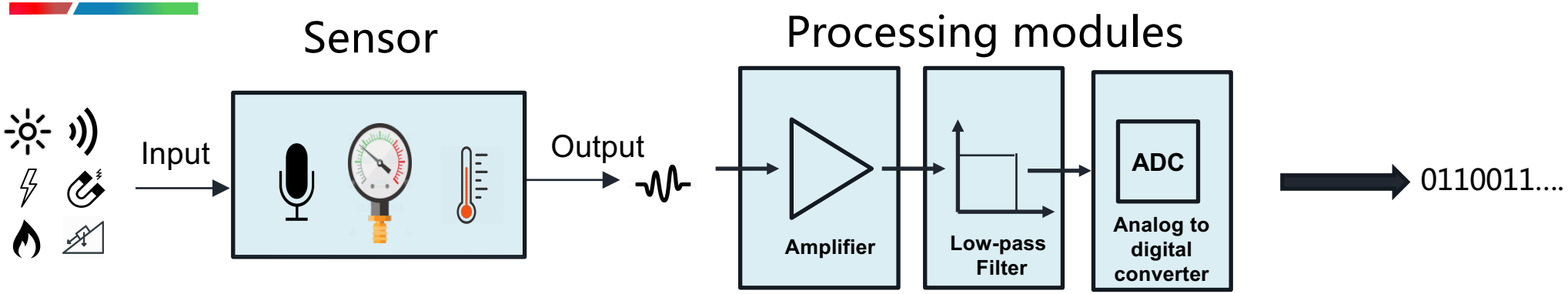


Pressure, acceleration, temperature, strain, or force

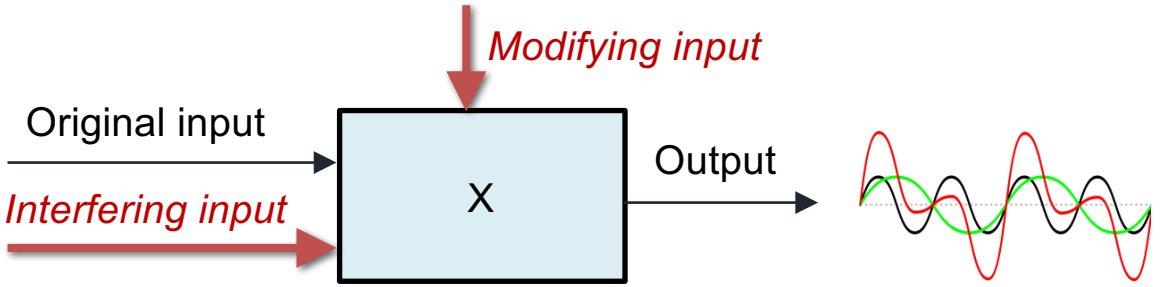
Strain-charge equations

$$\boldsymbol{S = sT + \delta^t E}$$
$$\boldsymbol{D = \delta T + \varepsilon E}$$

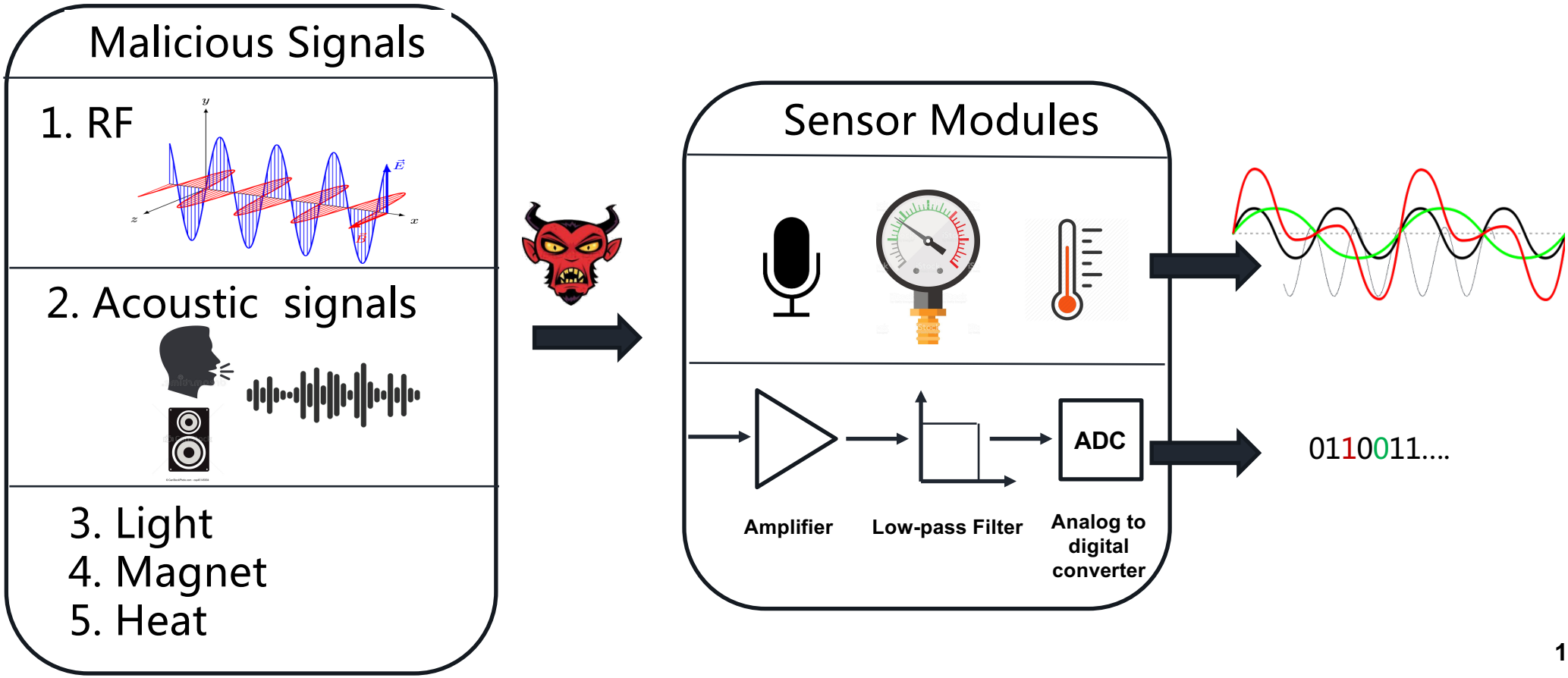
What is inside a sensor module



Physical signals -> Sensor -> Electrical signal



Can we trust the sensor readings?



ACOUSTIC SIGNAL INJECTION— VOICE ASSISTANTS

Dolphin Attacks: Inaudible Voice Commands
Guoming Zhang, Chen Yan, Tiancheng Zhang, Taiming Zhang, Xiaoyu Ji, Wenyuan Xu

Best paper at ACM CCS 2017


The New York Times

Alexa and Siri Can Hear This Hidden Command. You Can't.

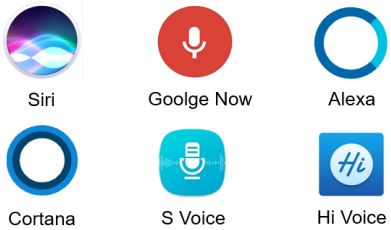
Researchers can now send secret audio instructions undetectable to the human ear to Apple's Siri, Amazon's Alexa and Google's Assistant.

How do voice assistants work?

Sound → *Electrical signal* → *Command*

Voice Command Input

Speech Recognition

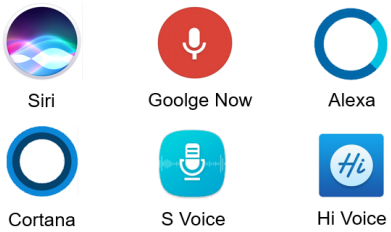


Command Execution

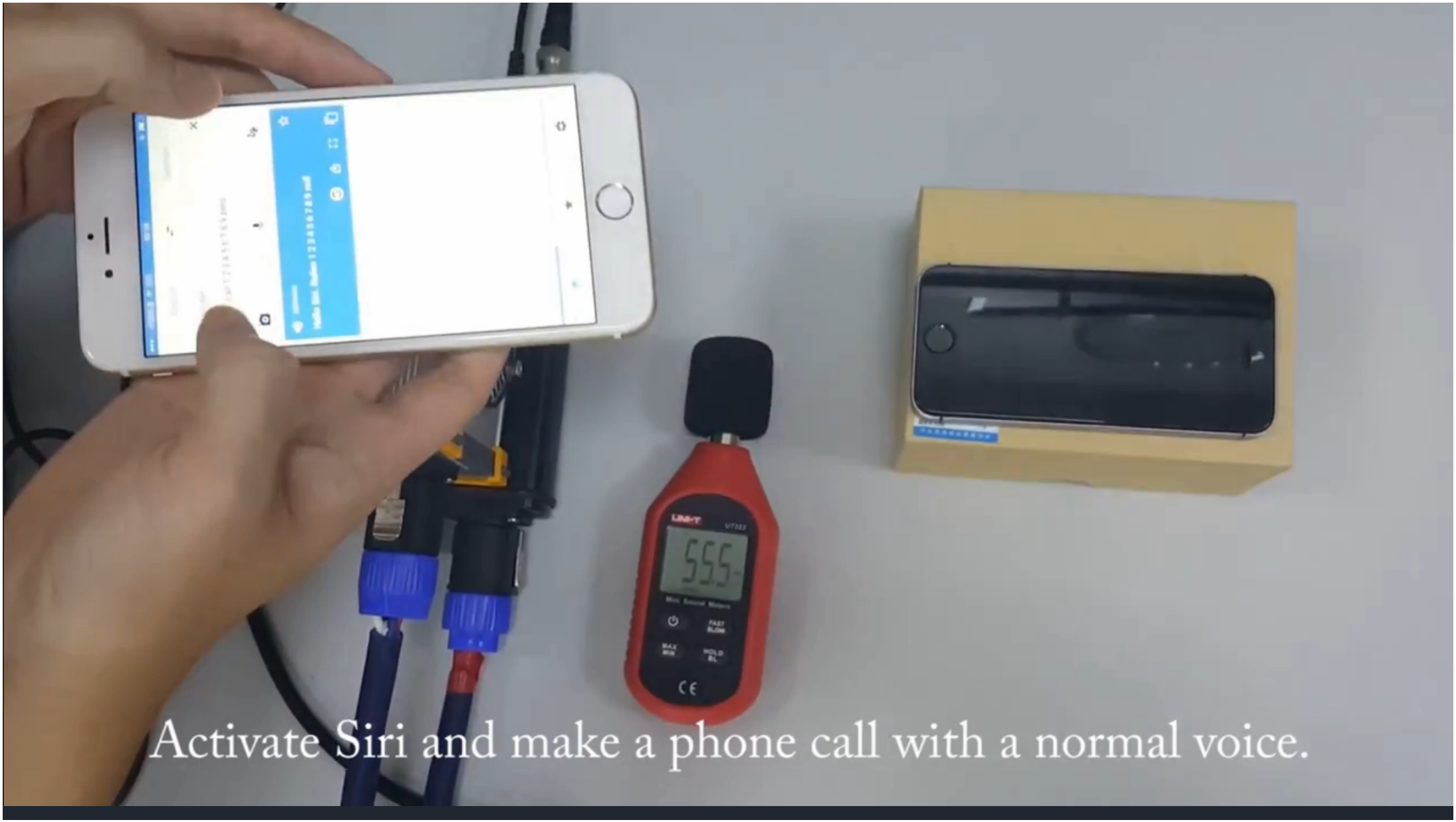
How do voice assistants work?

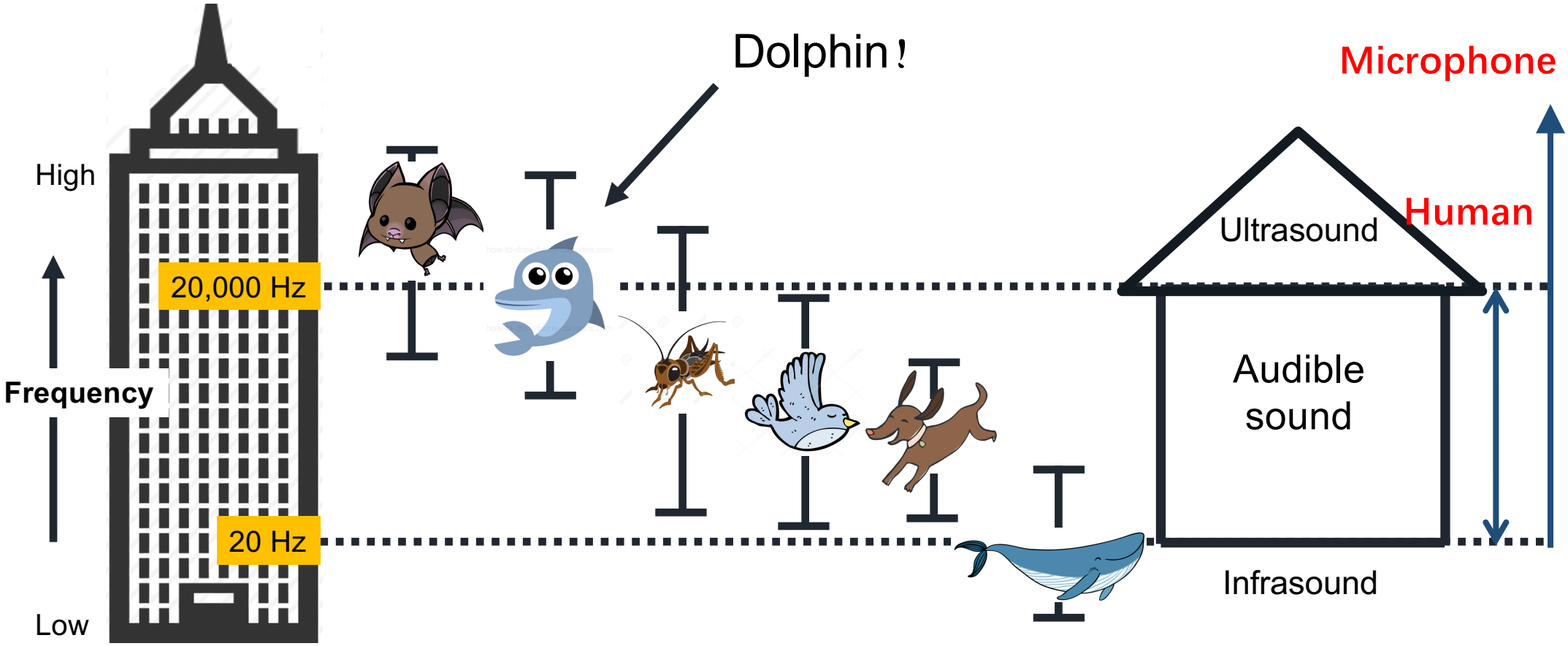
Voice Command Input

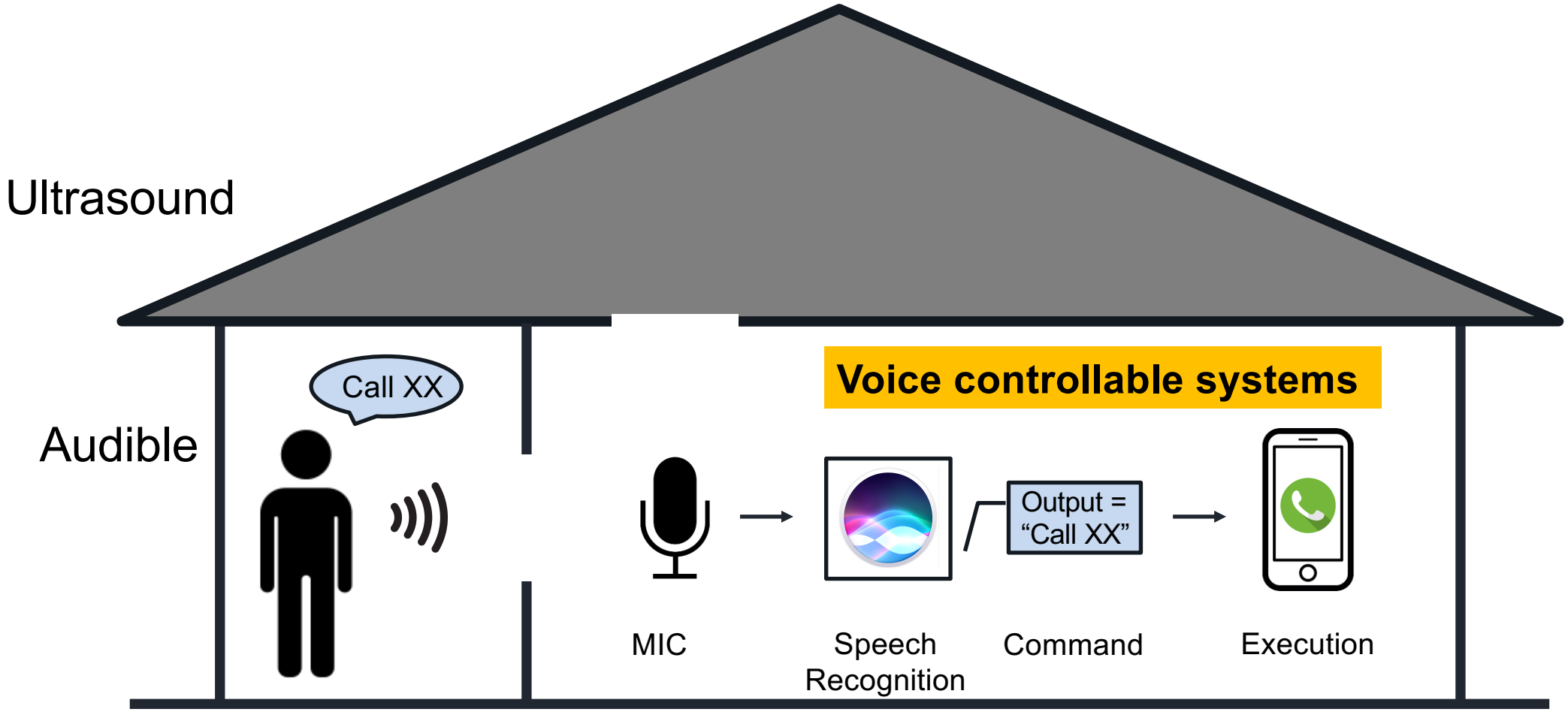
Speech Recognition

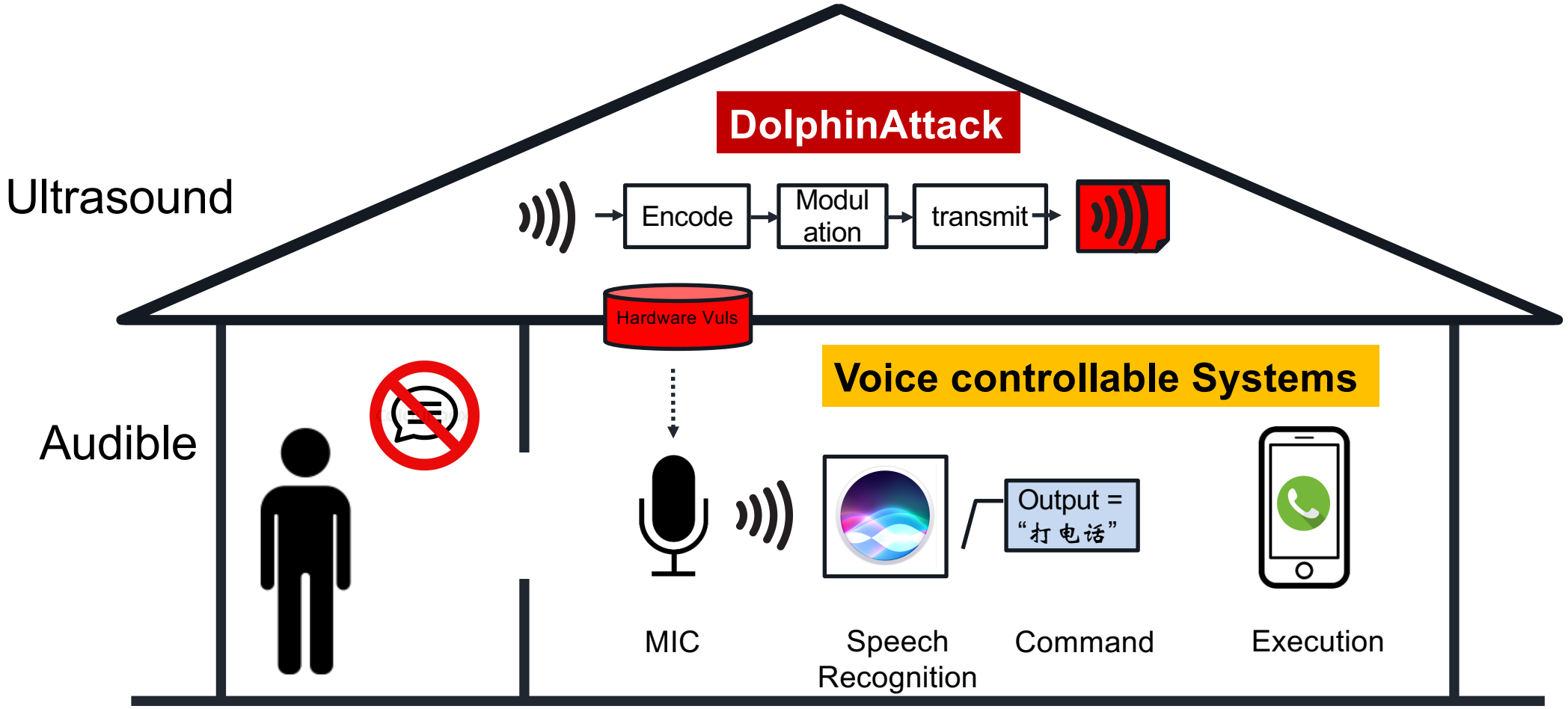


Command Execution

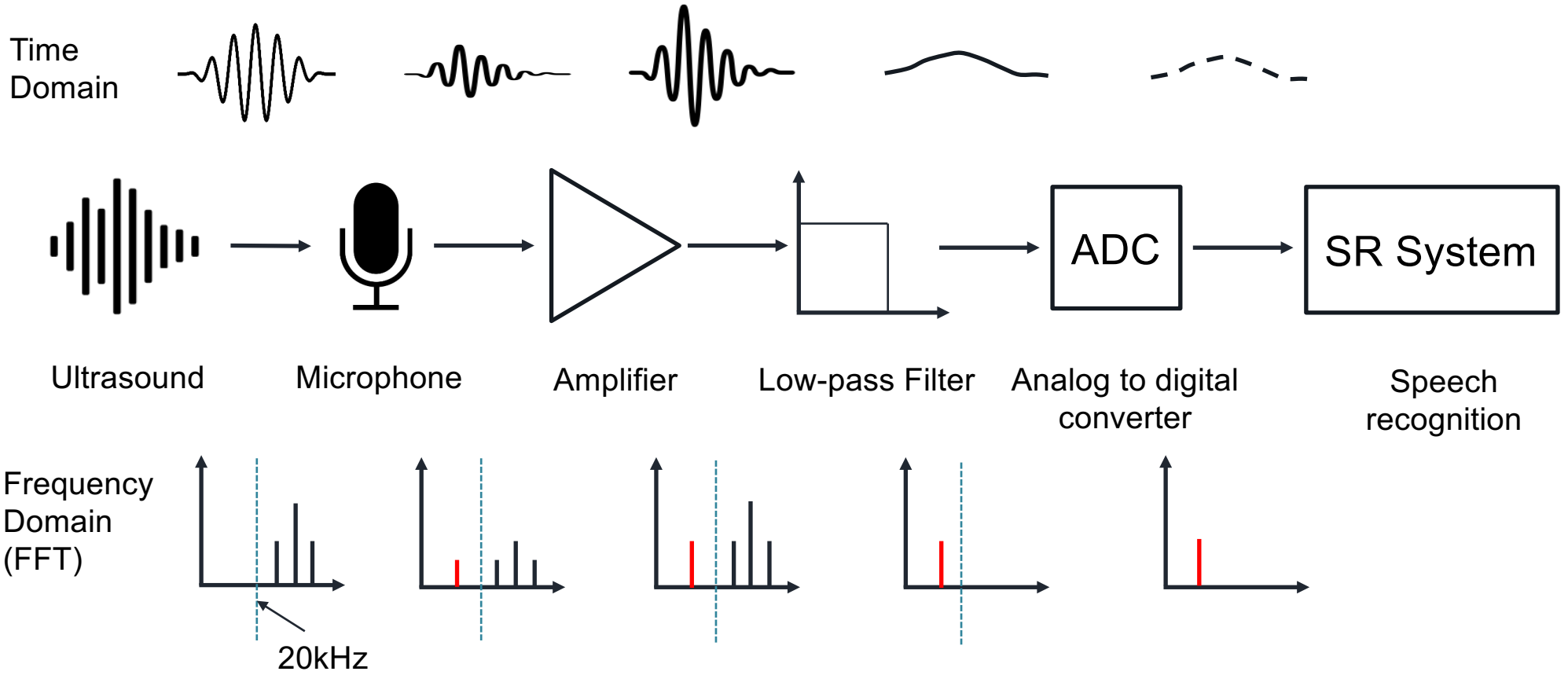

Activate Siri and make a phone call with a normal voice.


Dolphin!
Microphone
High
20,000 Hz
Frequency
20 Hz
Low
Ultrasound
Human
Audible sound
Infrasound

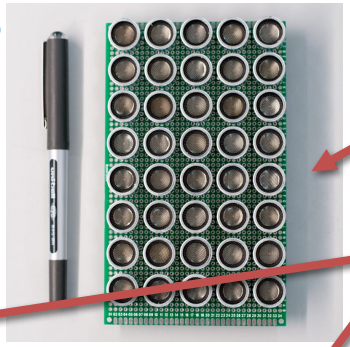

Ultrasound
Audible
Call XX
Voice controllable systems
Output = "Call XX"
MIC
Speech Recognition
Command
Execution

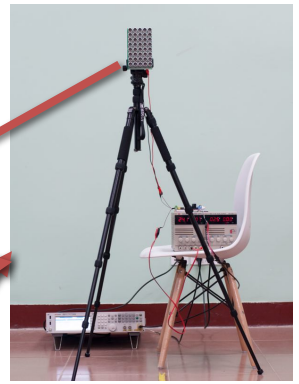

DolphinAttack
Ultrasound
Encode
Modul ation
transmit
Hardware Vuls
Voice controllable Systems
Audible
Output = "打电话"
MIC
Speech Recognition
Command
Execution

Signal Flow of DolphinAttack

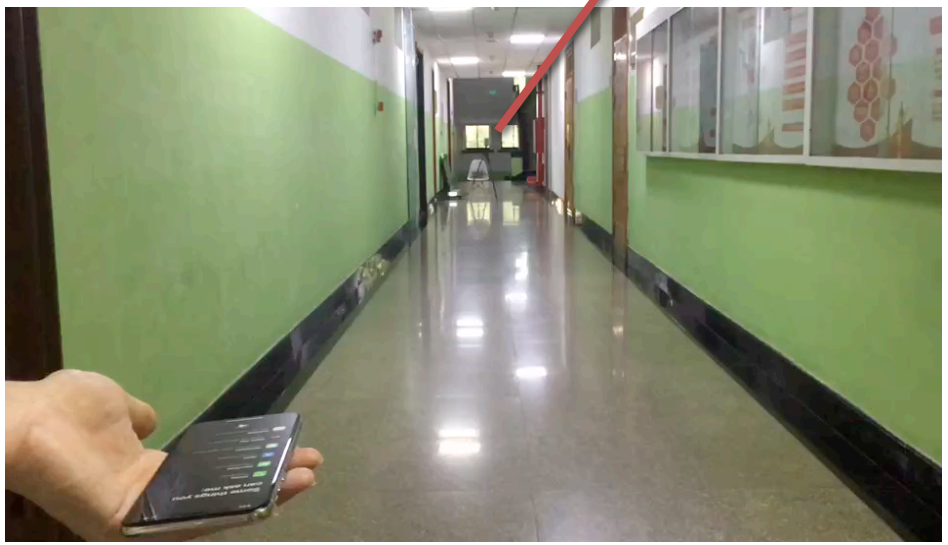


Can we boost the attack range?





10 meters



20 meters

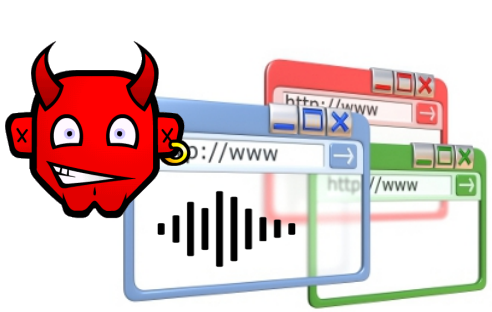
浙江大学 ZHEJIANG UNIVERSITY

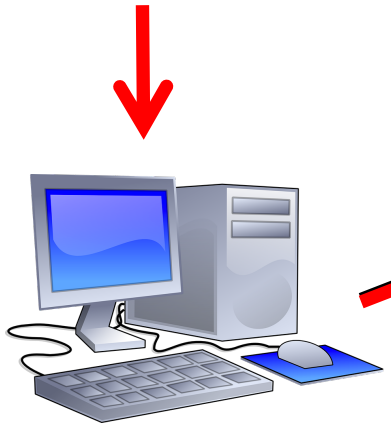
智能系统安全实验室 UBIQUITOUS SYSTEM SECURITY LAB.

DolphinAttack

ATTACKED DEVICE: APPLE WATCH

Attack Scenario: Remote Attack





Computer

Commodity Speaker

Smart devices


"Facetime 1551072xxxx"
Under attack

浙江大学 ZHEJIANG UNIVERSITY

27TH USENIX SECURITY SYMPOSIUM

智能系统安全实验室 UBIQUITOUS SYSTEM SECURITY LAB.

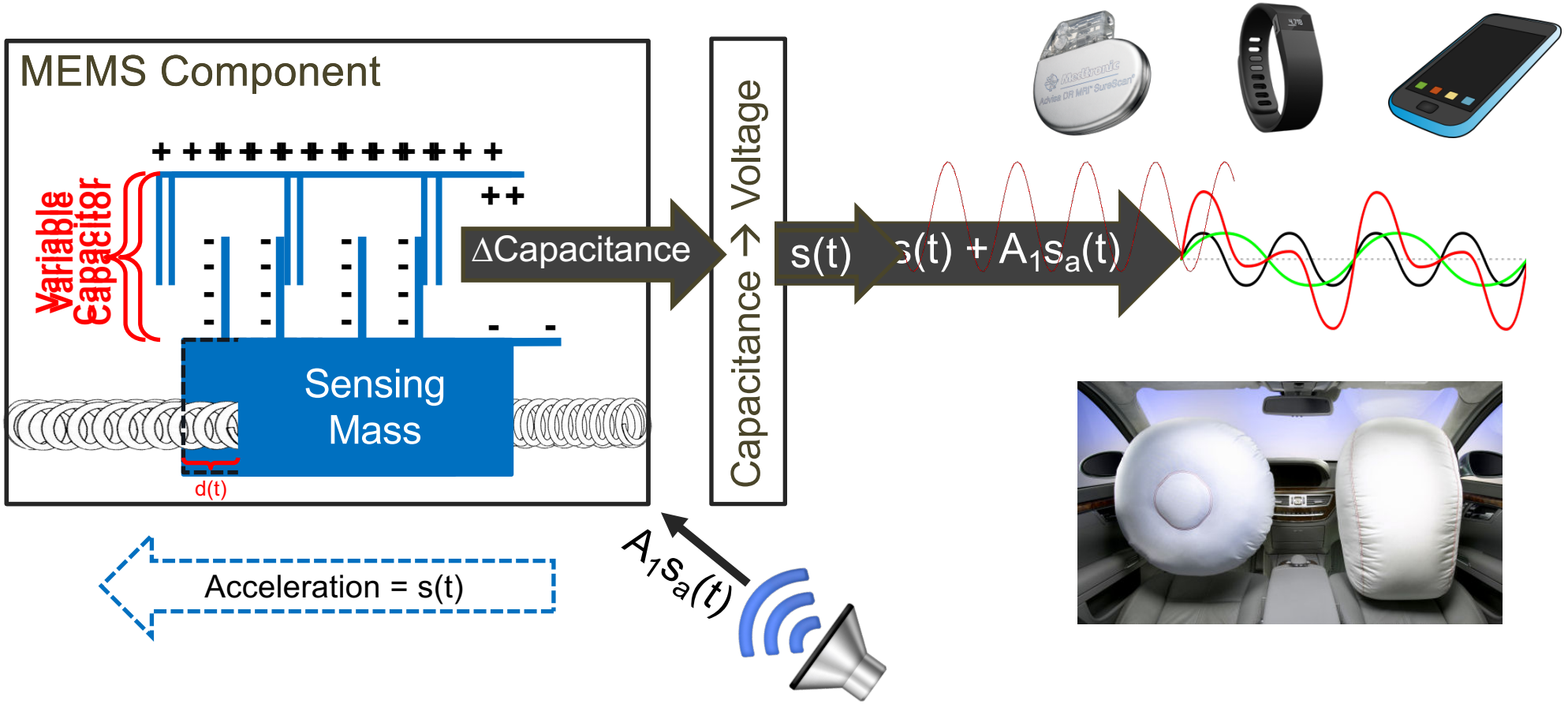
SENSOR SECURITY— MEMS SENSORS

WALNUT: Waging Doubt on the Integrity of MEMS Accelerometers with Acoustic Injection Attacks

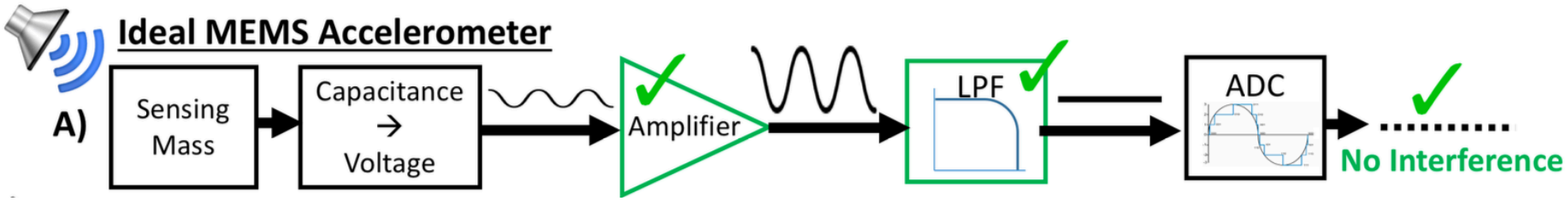
Timothy Trippel, Ofir Weisse, Wenyuan Xu, Peter Honeyman, Kevin Fu

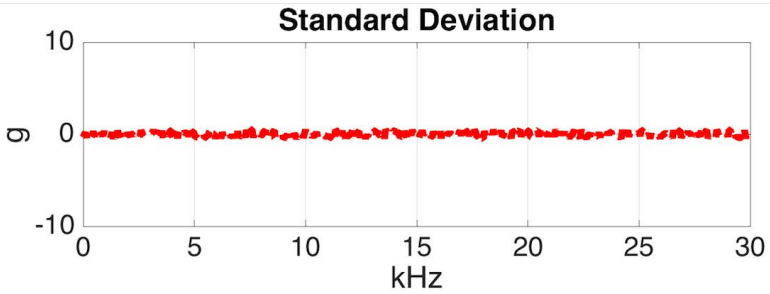
IEEE European Symposium on Security and Privacy

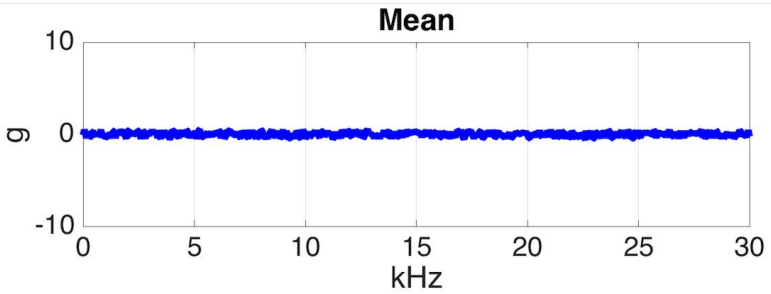
MEMS Sensors （Accelerometer）

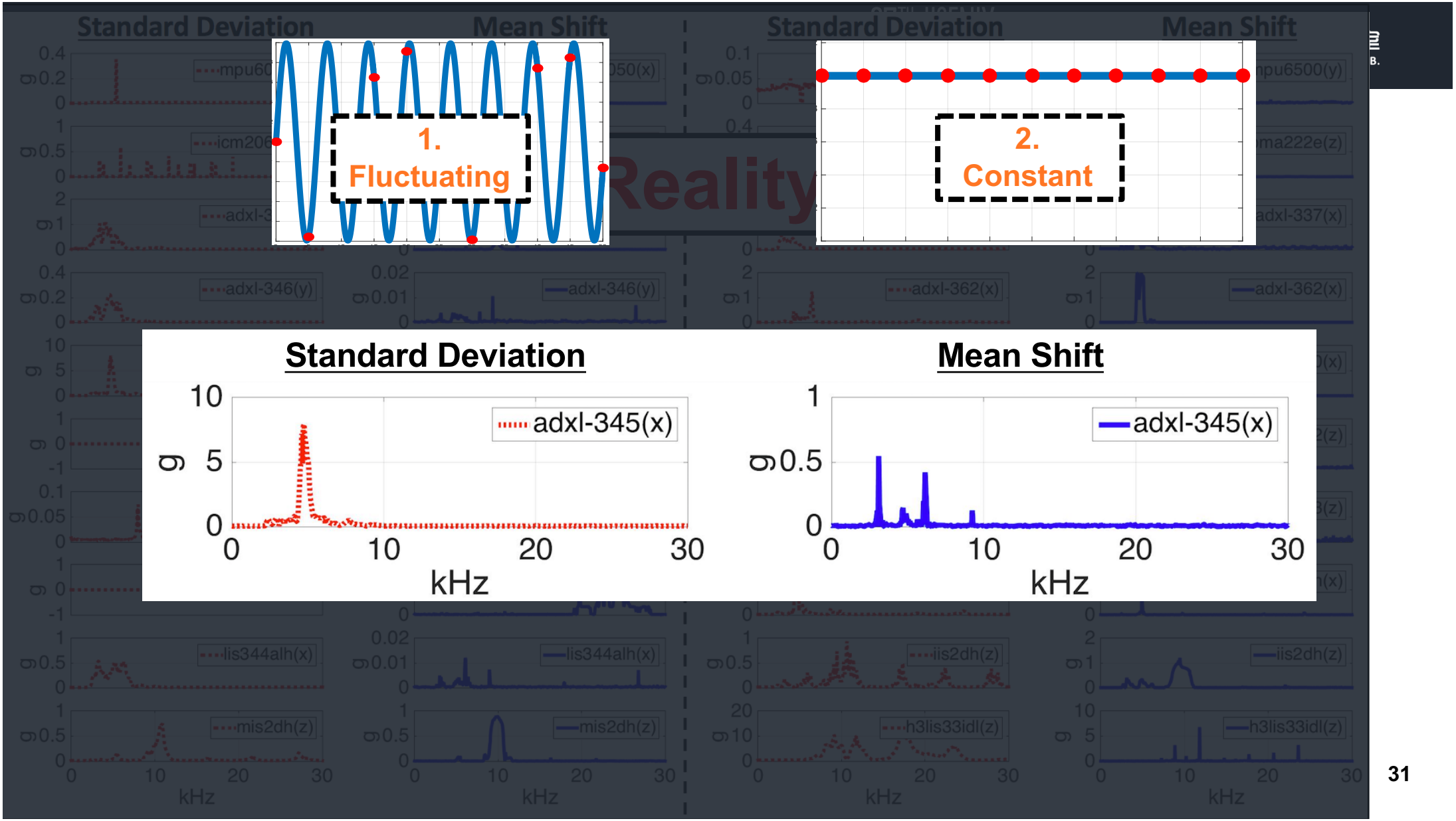


Ideal Accelerometer

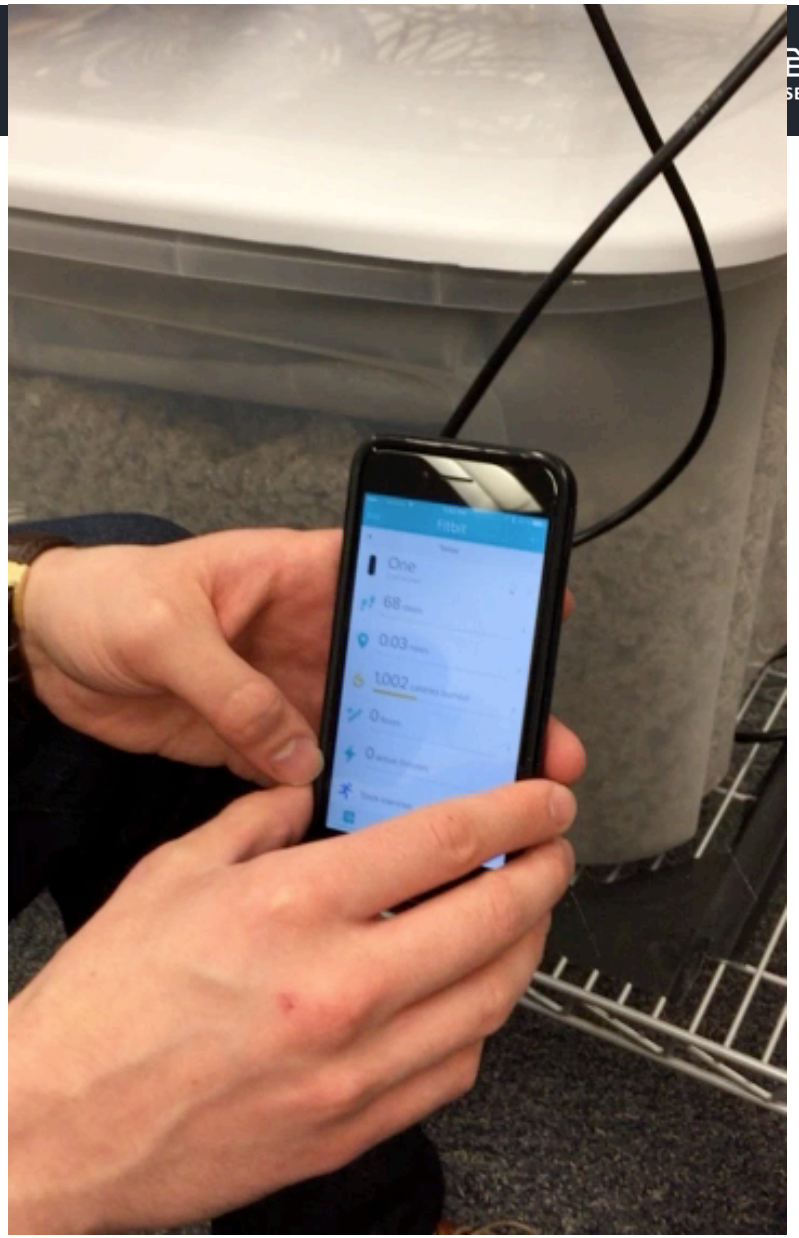




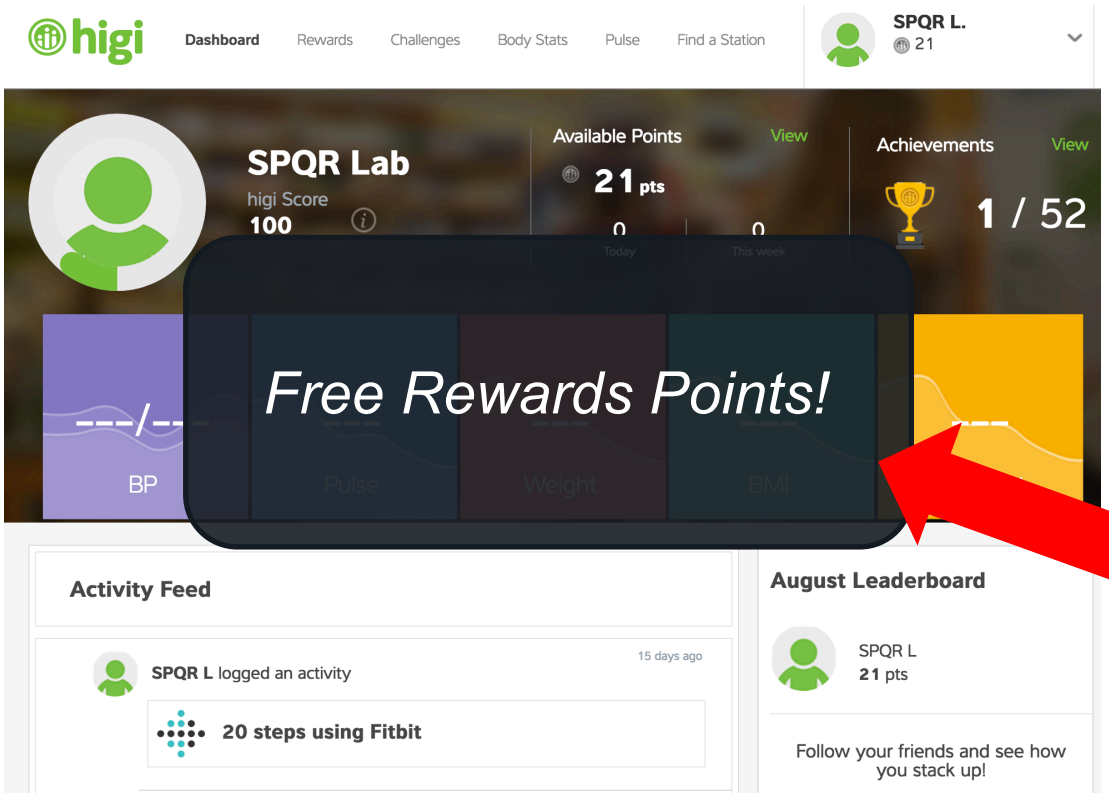



Standard Deviation
Mean Shift
Standard Deviation
Mean Shift
1.
Fluctuating
2.
Constant
Reality
Standard Deviation
adxl-345(x)
g
kHz
Mean Shift
adxl-345(x)
g
kHz

Free Fitbit Steps!



Fitbit Rewards



浙江大學 ZHEJIANG UNIVERSITY

27TH USENIX SECURITY SYMPOSIUM

智能系统安全实验室 UBIQUITOUS SYSTEM SECURITY LAB.

HARD DRIVE

Blue Note: How Intentional Acoustic Interference Damages Availability and Integrity in Hard Disk Drives and Operating Systems

Connor Bolton, Sara Rampazzi, Chaohao Li, Andrew Kwong, Wenyuan Xu, and Kevin Fu

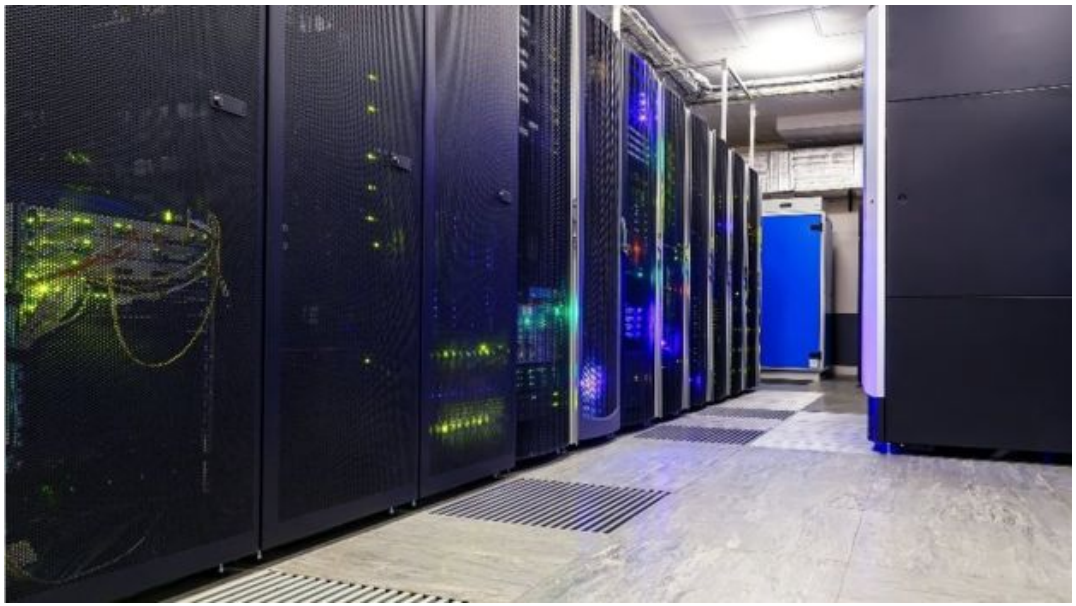
IEEE Symposium on Security & Privacy, 2018

Fire Drill Knocks ING banks data center offline

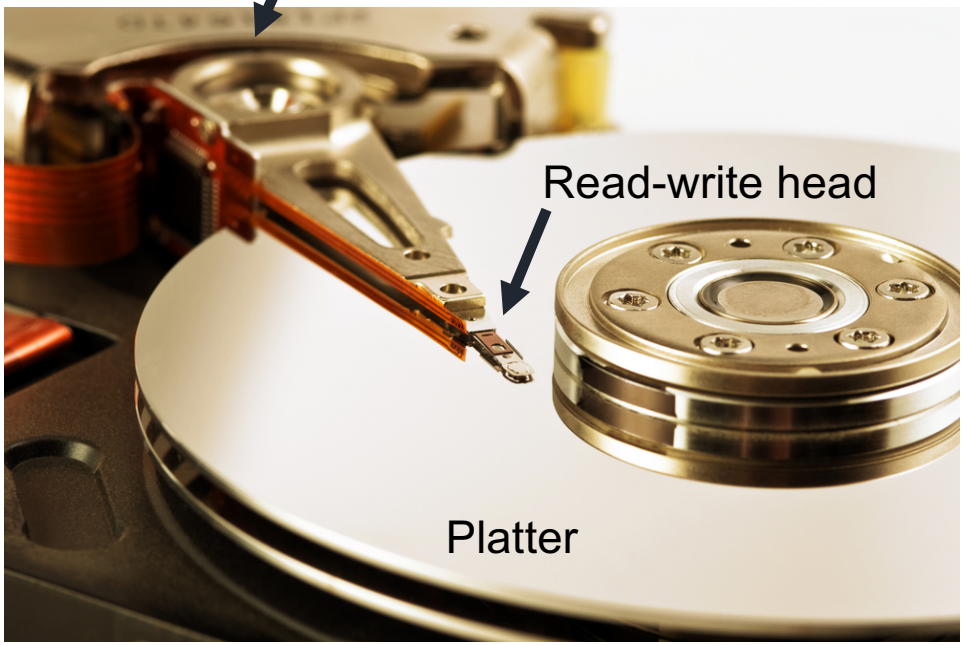
BBC NEWS

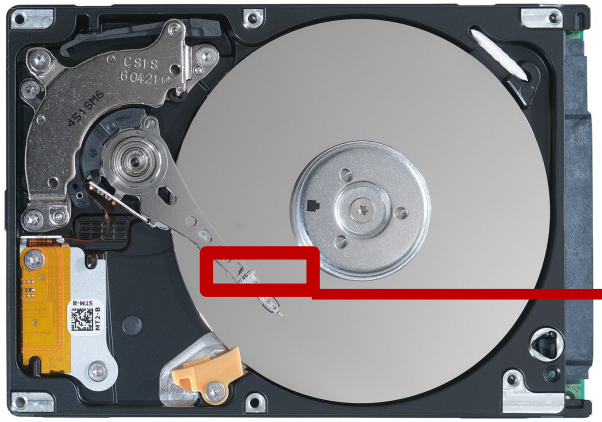
Technology

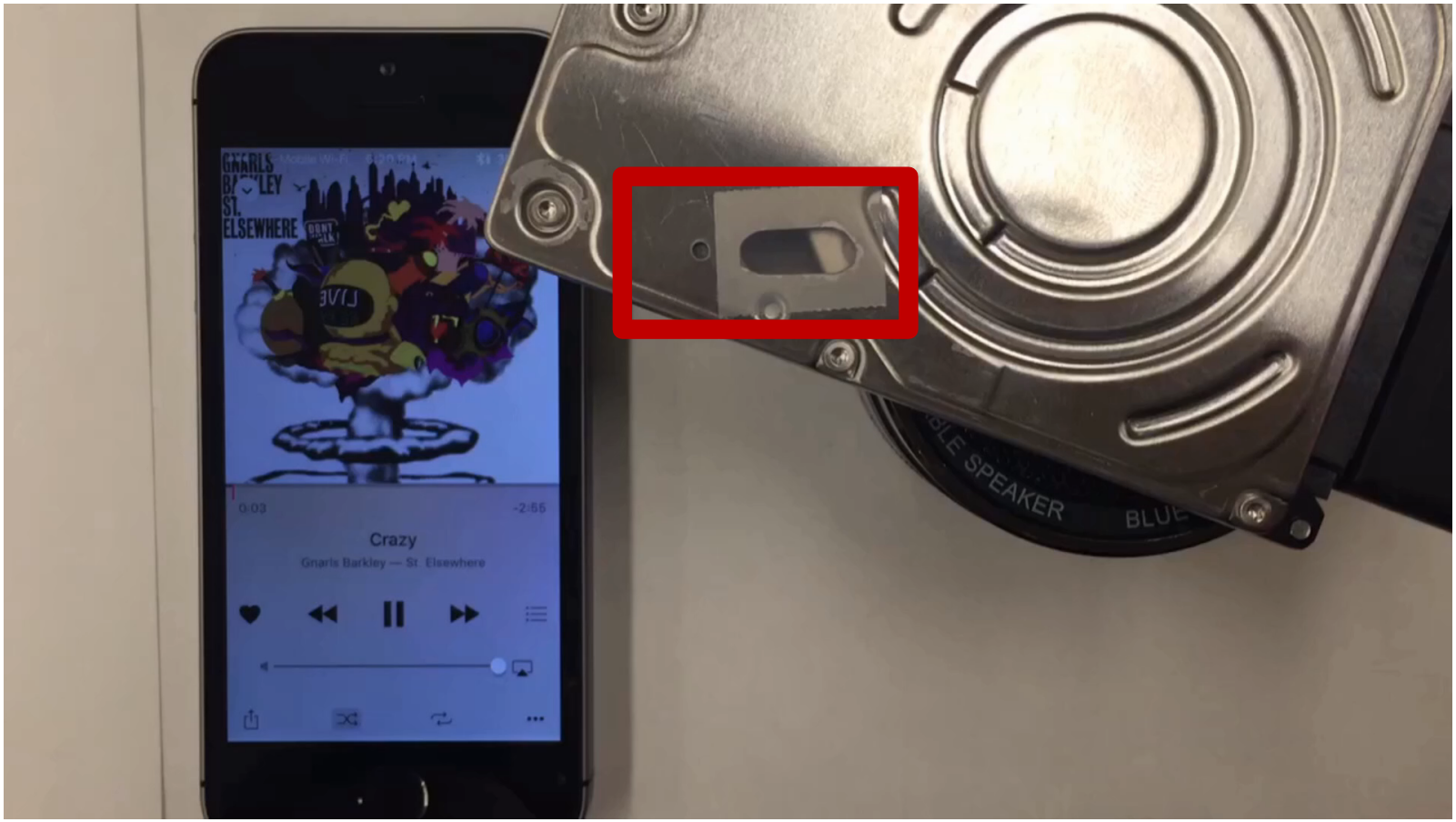
Fire drill knocks ING bank's data centre offline



Hard Disk Mechanics





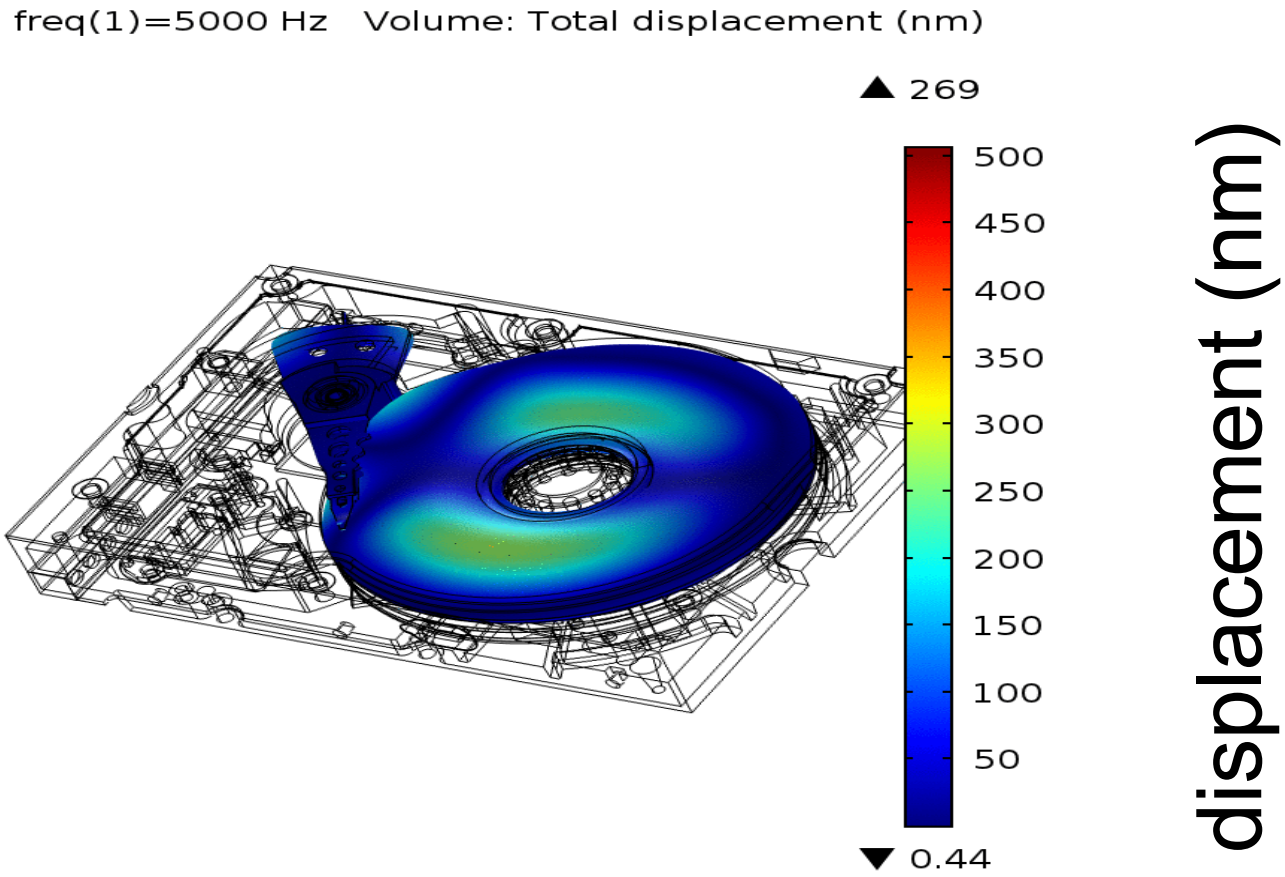

Crazy
Gnarls Barkley — St. Elsewhere
0:03
-2:55

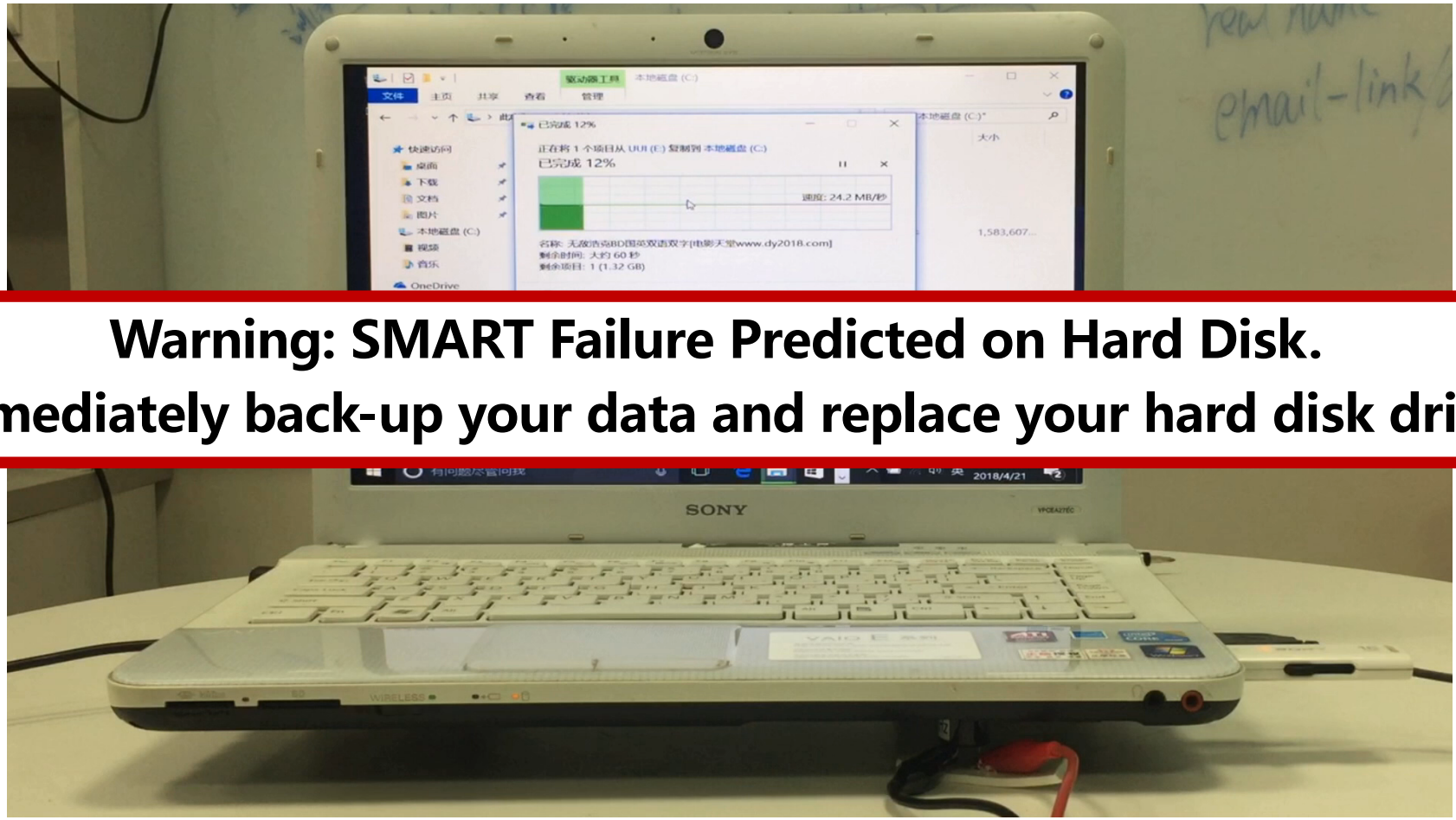
Threat Model

Ultrasonic transducer:
https://www.vellemanstore.com/en/velleman-ma40a5r-40khz-ultrasonic-sensor-transducer-receiver

Sound Distorts the HDD

Comsol Simulation
5 kHz (resonance)
120 dB SPL source
70 dB SPL at disk




Warning: SMART Failure Predicted on Hard Disk.
Immediately back-up your data and replace your hard disk drive
SONY

Case Study: Video Surveillance

80 seconds of video are missing

Conclusions: Analog is the new digital

- Analog security risks
  - Analog Sensors --- RF
  - MEMS Sensors --- Acoustic
  - Active Sensors --- Sensing principle

- Solutions
  - Microprocessors should not blindly trust sensors
  - Rethink ICs and hardware-software APIs

USSlab→ IoT Security

Join us!

- Tenure position
- Postdoc
- Summer interns

wyxu@zju.edu.cn

http://www.usslab.org/